﻿Section A 性能评估

主要通过拒真率（FRR, false rejection rate）和认假率（FAR, false acceptance rate）来对实验结果进行评估。

FRR：使用同一用户的指纹特征二进制编码序列作为PUF模型的输入，得到输出结果，两者间汉明距离大于等于阈值T的概率。

FAR：使用不同用户的指纹特征二进制编码序列作为PUF模型的输入，或者使用不同的可穿戴设备(PUF模型)处理同一用户的指纹特征二进制编码序列，得到输出结果，两者间汉明距离小于等于阈值T的概率。

FRR和FAR都用到了汉明距离，两个二进制序列间的汉明距离定义如下

﻿其中，和为二进制序列，,为序列中第i位的值，如序列”01001000”和”00101000”间汉明距离为2。越大，两个二进制序列间的差异性越大。

指纹特征通过传感器获得，经过二进制编码器后得到其二进制编码序列。指纹二进制编码序列作为PUF模型的输入，产生对应的响应。经10000轮认证测试，协议的FRR如图1所示。可看出，FRR随着阈值的变小而升高。

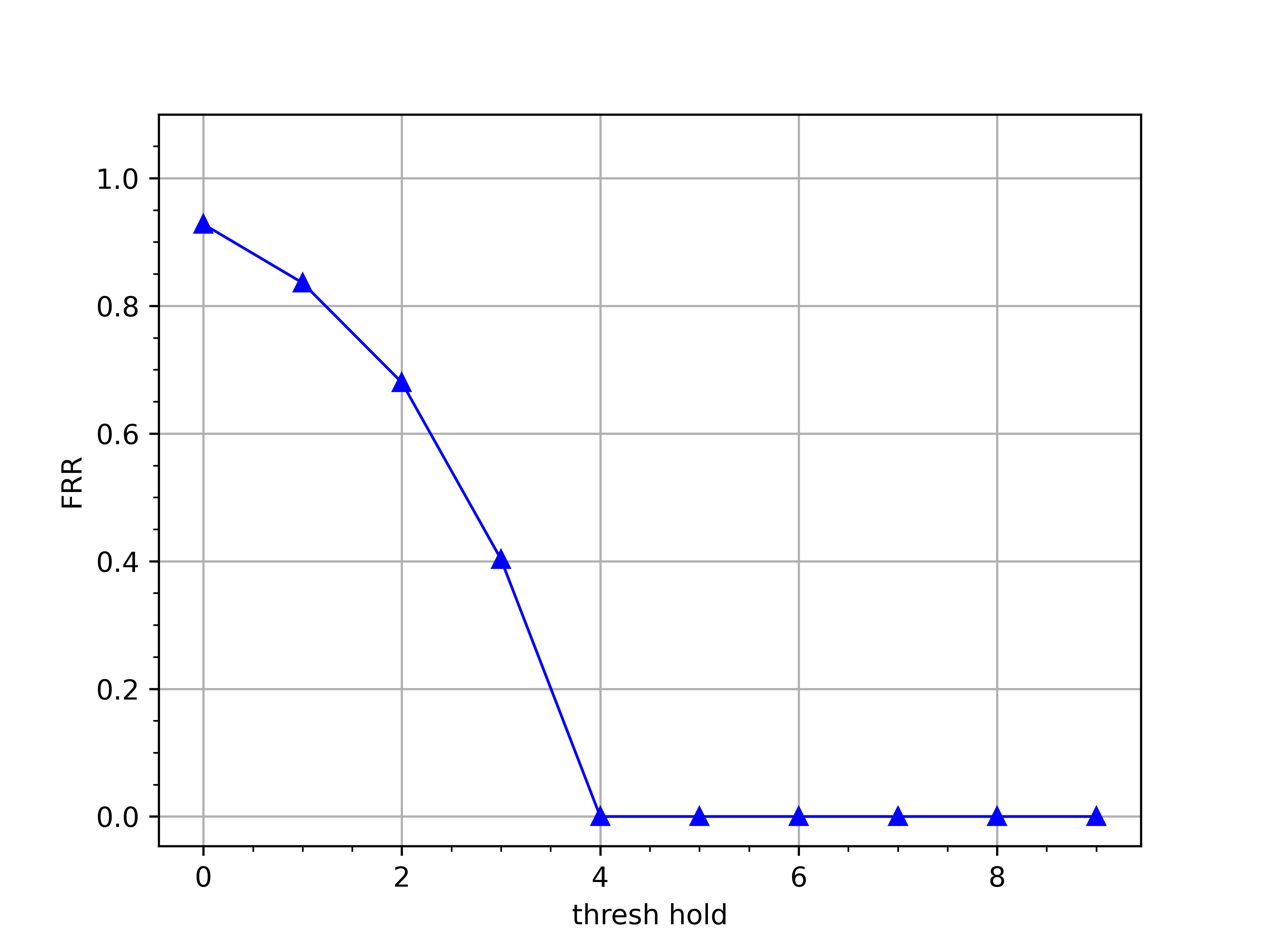


图 1 FRR

协议的FAR如图2所示，分为两种情况。第一种情况，使用不同用户的指纹特征二进制编码序列作为同一PUF模型的输入，共有10名不诚信用户参与测试，每个不诚信用户进行1000次认证。第二种情况，使用同一用户的指纹特征二进制编码序列，作为不同设备的PUF激励输入，共进行10000次认证测试。可看出，FAR随着阈值的变小而快速下降。

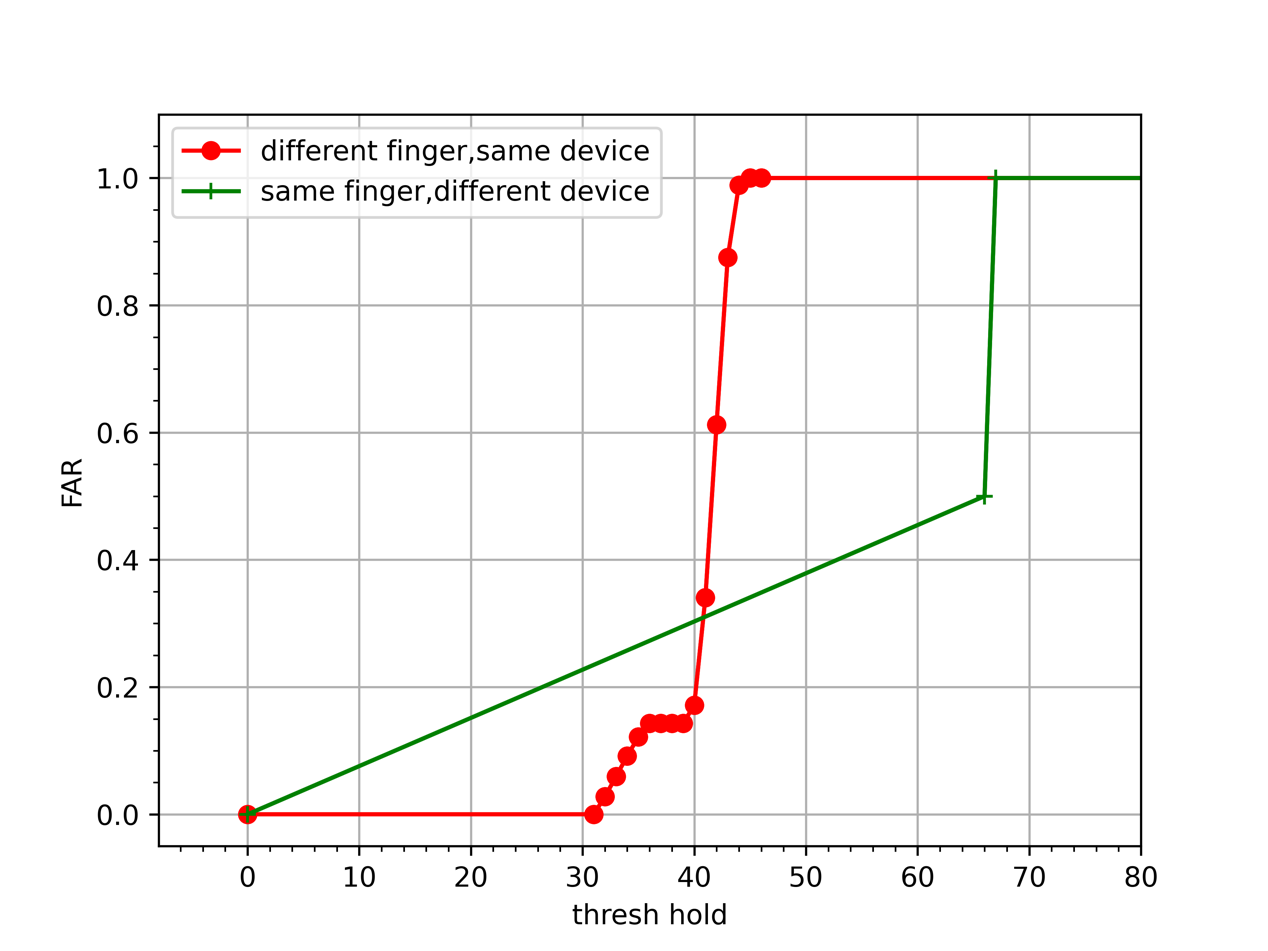


图 2 FAR

Section B 性能评估

现对DFAP(Dual Factor Authenticate Proctol)安全性进行分析，主要包括妥协攻击，假冒攻击和重放攻击。

妥协攻击利用体域网妥协节点向数据中心发送错误信息，将危机用户安全。在DFAP中，采用双因子进行认证，认证节点必须基于PUF和真实用户的指纹特征才能认证成功。假设体域网中某节点对敌手妥协，如某个丢失的传感器被敌手获得，然而敌手发起的认证将会失败，因为妥协节点不能获取真实用户的指纹特征。

假冒攻击利用体域网外部节点假冒正常节点，从而窃取用户生物特征，欺骗数据中心。一个非法节点潜入用户体域网并假冒成一个合法节点，在这种情况下，非法节点只能提供用户的指纹特征，而不能提供有效的物理设备特征，最终认证失败。

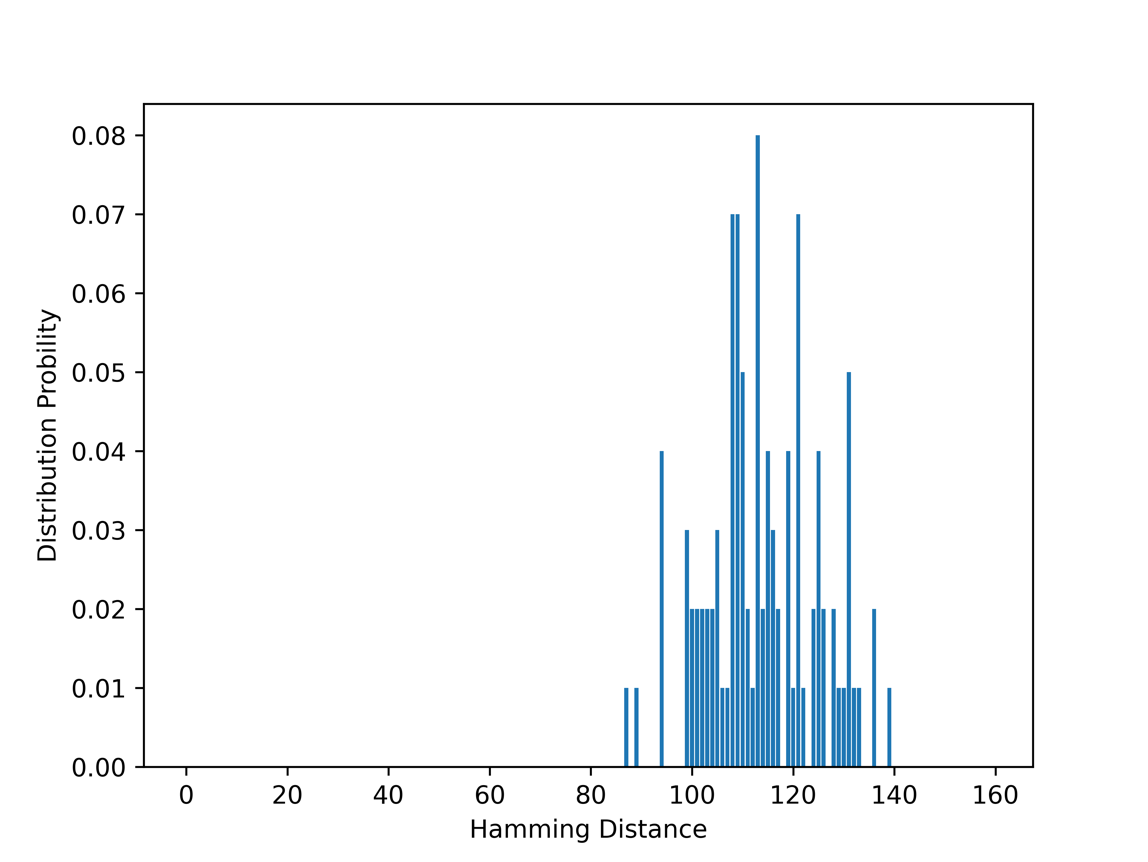
重放攻击利用一个有效数据重复传输以欺骗系统。利用重复信息，敌手试图非法进入应用系统。在DFAP中，指纹特征为实时数据，不同时刻获取到的指纹特征都不完全相同，历史或将来数据不同于实时数据。同时，指纹特征二进制编码序列间的差异将导致生成的PUF响应产生变化。同一用户的异步指纹特征二进制序列间汉明距离的概率分布如图3所示，这表明，即使对于同一指纹，每次采集后序列化的结果也存在着较大差别，故生成的PUF响应间也存在着较大差别。因此，利用重复信息认证失败。

图 3 同一用户异步指纹特征二进制序列间汉明距离的分布概率

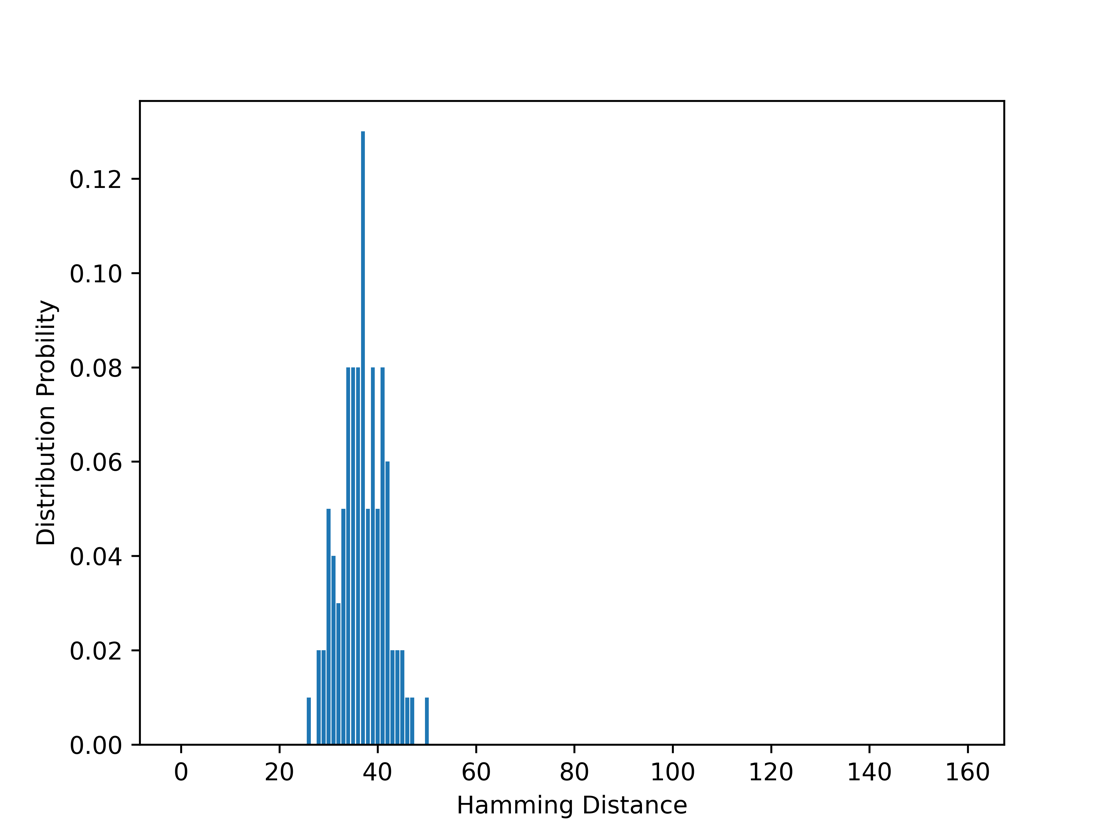


图 4 指纹特征二进制序列间不同汉明距离下的PUF响应间汉明距离分布概率